SUBMISSION NO. 29

FORTINET®

Inquiry Into Cyber Crime

Response prepared by Fortinet

June 2009

Preface

Cybercrime is a global phenomenon that has widespread implications to Australian businesses and consumers alike. The continued growth of online business has fueled online crime and has put anyone that does business on the internet at risk.

This paper has been prepared with a local focus to the Australian economy with reference to the:

- nature of online threats,
- implications,
- level of understanding and awareness,
- evaluation of the current measures employed by the government,
- further initiatives to aid in combating cybercrime,
- emergence of new technology that may aid in combating online crime.

The results of this study are set out in the following pages. In preparing this document, Fortinet reviewed the current status of online crime, and used it's resources in researching this information. Main sources of information for this paper came from Fortinet Security Threat Research and Response teams.

This paper presents Fortinet's views, based on our research and discusses what is happening now and what may happen in the future.

Charlie Cote, Regional Director, Fortinet
ccote@fortinet.com
02 8007 6001

June 2009

Contents

- Overview
- Nature and Prevalence
- Implications
- Awareness
- Measures to Combat Cybercrime
- Future Initiatives & Emerging Technology

Overview

Where we were once protected and isolated over vast distances and the security of a lock and key, the online world has broken down barriers of distance and time and allowed for an almost infinite medium to deliver and execute new business ideas and partnerships.

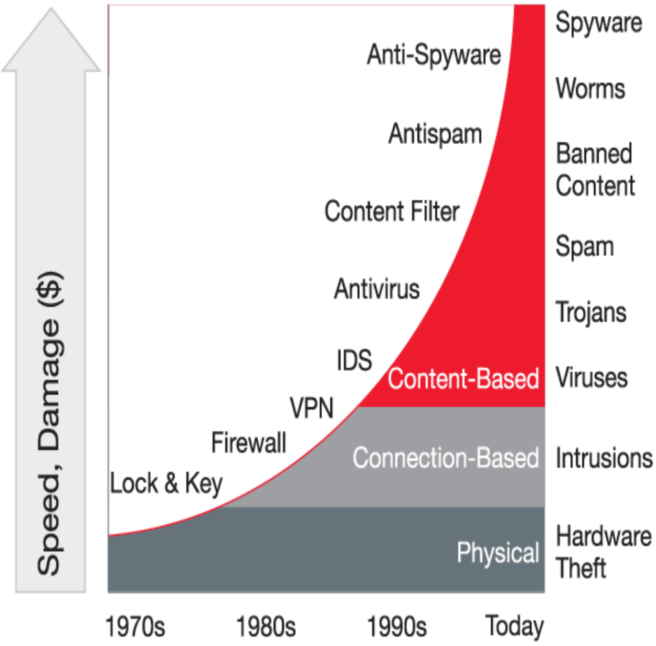
Unfortunately, the new face of crime has reared it's ugly head on the world of online business. Once relegated to the world of expert researchers and institutions, the internet, has now become a fast, profitable and consistent money earner for organized crime and individual criminal elements.

These individuals and organizations are executing these crimes using the internet, which provides an excellent layer of anonymity. They use computers as their weapons to execute crime by exploiting weaknesses in common computer operating systems and applications that run on them.

A very common target in these attacks are consumers and businesses that host or maintain information on their computer systems. Financial and personal information is the typical target in many instances, while in others, the attackers hope to take control of their target so that they can execute further criminal activities anonymously.

While cybercrime itself is not new, the methods used to execute it's activities evolve, playing cat and mouse with legal authorities sought out to stop them just as with regular crime.

The threat to the Australian economy is real. Defending against these criminal threats will require a layered defense at all levels of public and private sector business as well as an unwavering information campaign to educate the general public against these criminal elements.



Nature and Prevalence

The nature of most attacks in Australia as observed by Fortinet's research teams appear to be widely distributed attempts at compromising any computer that is online.

These attacks aim to take control of host computer and leverage it's resources to further exploit other machines or execute criminal activity.

The most prevalent detection local to Australia was a Trojan Downloader which was first discovered on May 19, 2009. In such a short time frame since discovery, 12 days to be exact, this threat easily became Australia's most prevalent threat for 2009. Table 1 below shows a summary of detected threats for Australia.

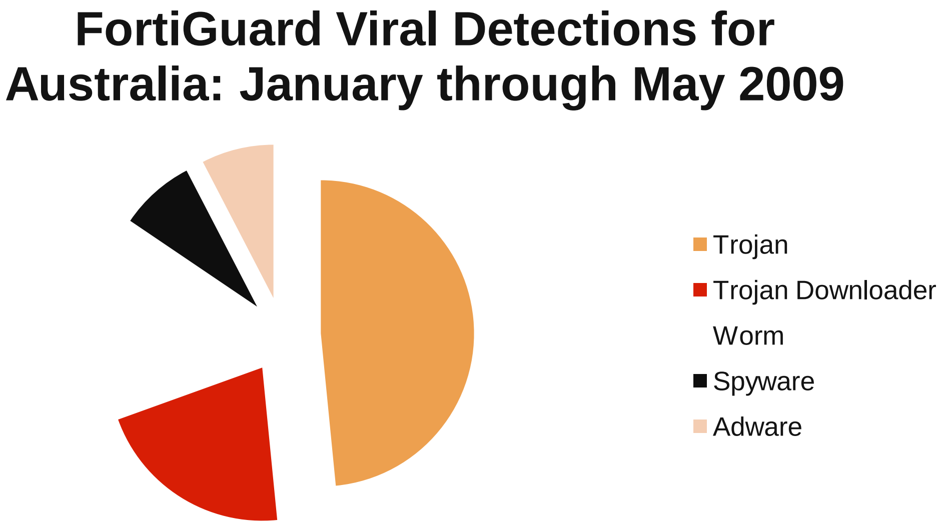


Figure 1: *Australian Threat Detections, January 1 – May 31 2009*

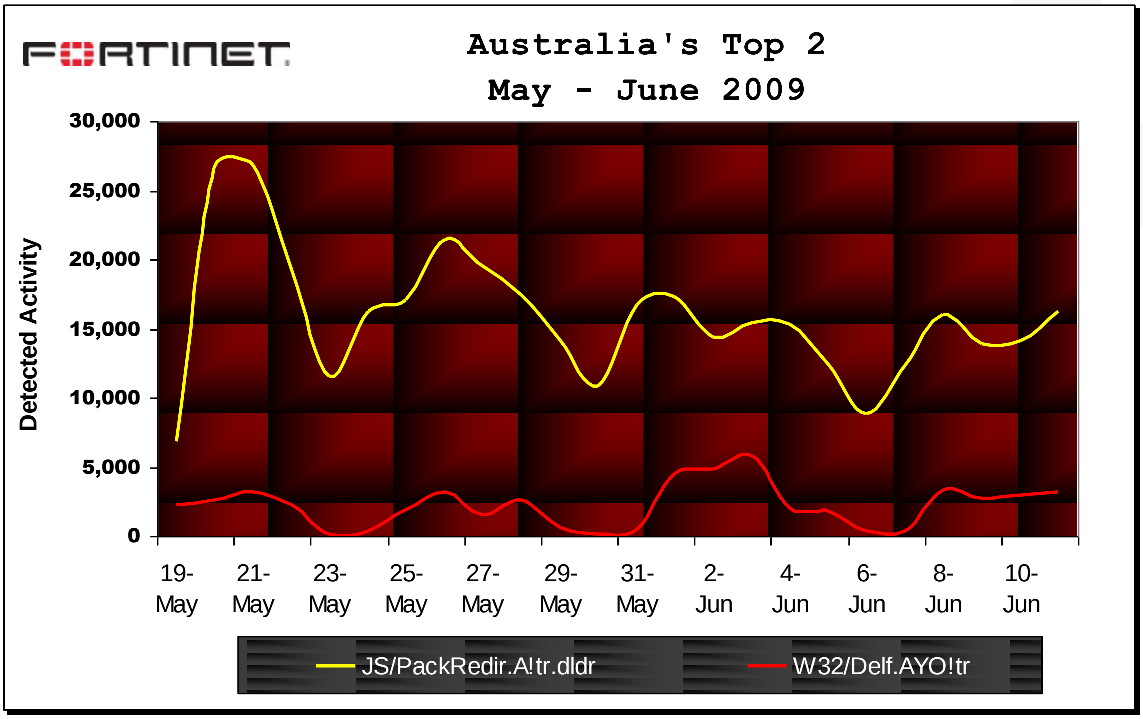


Figure 2: *A snapshot comparing Australia's No. 1 and No. 2 most prevalent threats for 2009*

Traditionally, many of these threats have been executed by remote hosts targeting other computers. In more recent times, the attacker looks to compromise a website and insert it's malicious software, thereby infecting vulnerable users visiting the website.

For example, when a victim visits an infected website, the software is executed and downloaded to the victim's computer. The victim user is then re-directed to a website which hosts malicious components, very commonly observed to be PDF and SWF files (Adobe Acrobat / Flash).

These files then take advantage of software vulnerabilities through the aforementioned components by exploiting vulnerable software. Downloader code as a result of this will obtain malicious software via remote sites, which is the behavior of a Trojan downloader. Figure 2 below graphs the activity of the two most popular Trojan Downloader in Australia.

A perfect example of how many threats have expanded to new and emerging platforms. Traditional infection vectors such as email are still quite prevalent, though not as dangerous as they were in previous years for several reasons:

1) Enhancement of Spam Filtering & Technology
2) Public Education and Awareness
3) Legal Action on Spam-Centric ISPs (McColo, 3FN/Pricewert)
    1) Enforcement of Can-SPAM Act (Facebook 2008)

Therefore, as more safe guards have been put in place to dilute the effectiveness of threats, cyber criminals have invested into emerging areas. Typically, they follow traffic – and most traffic from end users today is web sites and platforms such as social networking and blogs. One distinctive trait of threats today (next generation) is that their targets are two-fold, targeting both servers and clients. Often, these attacks are combined from a single campaign, as we can see with *JS/PackRedir.A!tr.dldr* Trojan Downloader.

Malicious components are often downloaded third party software or adware that aims to make profit for the originator of the attack. The combination of attack vectors, and use of downloaded malicious components, is precisely what defines modern threats that Fortinet sees and processes today: multi-pronged, multi-functional attacks. As new platforms arise, threats will follow as their use becomes popular.

The top five threats detected since January 2009 for Australia were Trojans by nature. This in general trend holds true world wide, as Trojans are frequently deployed. They are commonly used for to collect credentials (bank, online gaming, web servers) and other critical data.

Finally, targeted attacks (low in volume, premeditated) are an increasing attack front favored by cyber criminals. These typically use very precise information through, as an example, a phishing e-mail or social engineering scheme in order to deliver malicious code and compromise a victims machine. This is done through higher profile end points (C-level executives, etc) and is often referred to as spear-phishing.

Poisoned documents are often used in these attacks to deliver custom-built Trojans that leverage sensitive information. Thus, Fortinet has seen an increase in poisoned document attacks, both through the masses (blanketed attacks) and targeted attacks. Figure 4 below shows this trend.

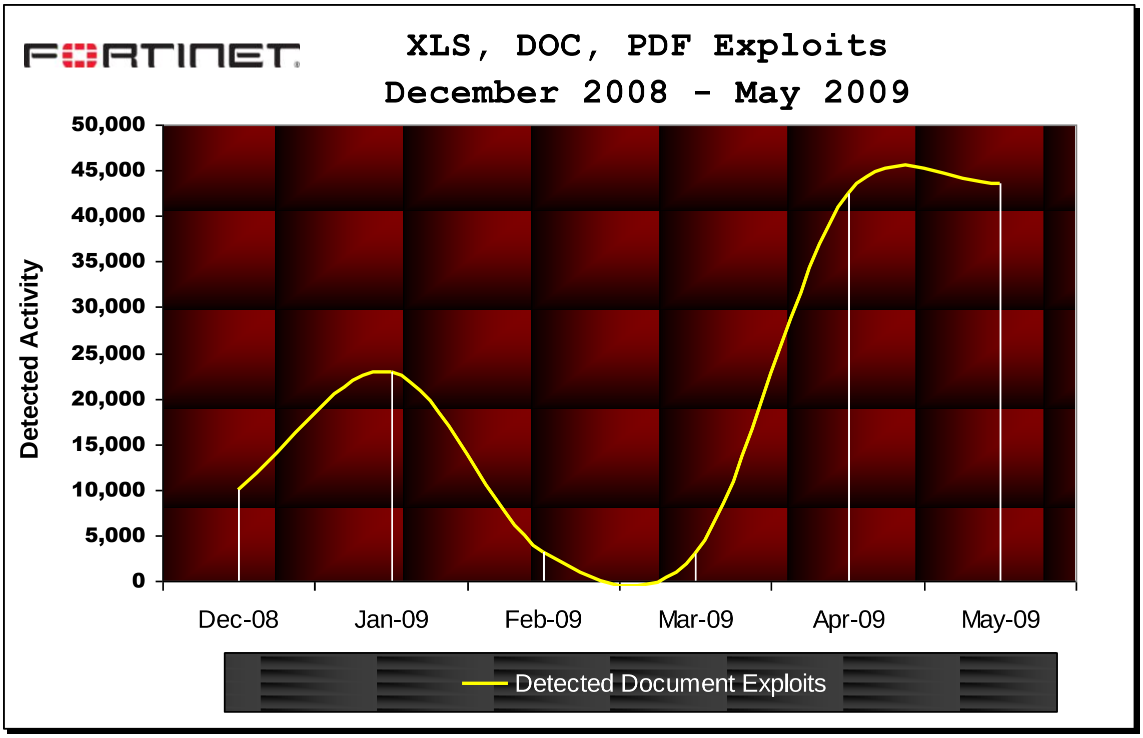


Figure 4: *Poisoned document detection showing attack curve*

Implications

Cybercrime poses risk to online business in Australia. Fortinet's research globally has indicated that online threats continue to proliferate as the criminals continue to search out ways to compromise their victims more easily and lower costs associated with exploiting/acquiring their targets.

One of their most profitable activities are botnets. The main economic impact of botnets is that of the digital underground. This economy flourishes thanks to spam campaigns to affiliate sites, driven by botnets. Botnets are often rented in the digital underground to launch these campaigns by a third party operator, or other attacks such as DoS (Denial of Service). These DoS attacks can directly impact the Australian economy by taking down public services such as banking. This has been witnessed before with the cyber attacks on Estonia and Georgia.

The security impact of botnets is of concern. Modern botnets are very resilient, and in some cases have been in operation for years. This is because of several complications:

1) Redundancy methodologies
   - a) Fast Flux Hosting
   - b) Peer to Peer

2) Safe Havens / Jurisdictional
   - a) ICANNN *(Internet Corporation for Assigned Names and Numbers)* Accredited Registrar Cooperation
   - b) Internet Service Provider Cooperation

3) Software Coding methodologies
   - a) Server side polymorphism
   - b) Common channel encryption / propagation

Botnet is a jargon term for a collection of software robots, or bots, that run autonomously and automatically.

Fast flux is a technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

Efforts have been made to take down botnets that are hosted through single point of failure channels (Command & Control), as witnessed with McColo in November 2008. Despite this, malicious threats using this end point simply migrated to other safe havens. Therefore, even single point of failure botnets that are not using peer to peer communication remain resilient to date. This is not welcome news since further advances have been made by cyber criminals to make their botnets robust.

International co-operation is necessary to allow authorities to 'take-down' the source of these attacks along with jurisdictional enforcement. Layered security, as discussed later, is the best approach to mitigate botnet threats due to multi-functionality and reasons mentioned above.

An example of an emerging, robust botnet is Waledac. Fortinet has been monitoring this threat closely since its inception (late 2008 / early 2009). Here are some key features of Waledac, a true next generation threat:

1) Peer to Peer Communication
    a) Client Mode (Accept Spam Templates / Spam Out)
    b) Proxy Mode (Proxy Spam Template Information, Host Web Campaigns)
2) Fast Flux Hosting
    a) Server Side Polymorphism
    b) Malicious code served changes every 30 minutes on server
    c) New infected hosts are re-packed into these variants, therefore updating a new seed list
3) Common channel encryption
    a) Communication through peer to peer network is done via HTTP
    b) Encrypted with dynamic session key

Waledac has used at least five high profile social engineering web campaigns. These host web sites through its infected proxies (#1b above), with malicious links that download further incarnations of the Waledac botnet (#3a above). As a final note to #4b, encryption has been used more frequently by cyber criminals for malicious acts (malencryption). This is used for covert reasons during communication, identification of malicious code (malicious updates), and more recently, ransomware.

Ransomware is a technique where documents and other important file data is encrypted by a remote malware author who holds the key to decrypt the information. To obtain the key, a fee is charged, thus placing the data up for ransom. We have not seen high volumes of this attack yet, but recent Ransomware code was observed to be downloaded by several Trojan variants. Ransomware, unlike most modern threats, is destructive and can cause a large impact to enterprise and government. Figure 5 below shows detected Trojan activity for 2009. A significant increase of this activity is due to online gaming Trojans, which target accounts for monetization – referred to as real money trading, or RMT.

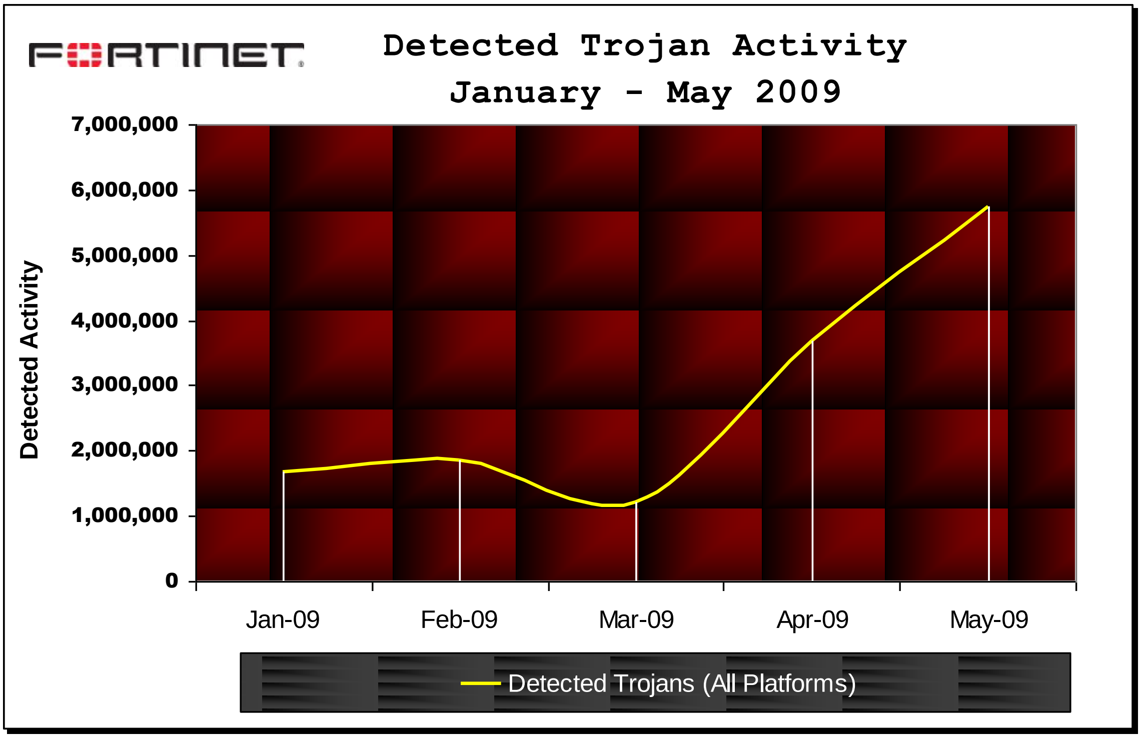


Figure 5: *Detected Trojan activity for the first five months of 2009*

Awareness

Understanding and awareness of e-security risks within Australia’s borders is as challenging locally as it is internationally. With the internet is still growing and new users (business and consumer) are going online everyday, there exists a significant gap in knowledge and understanding of the exact nature of threats to the average consumer.

The problem is two fold. Existing users must be educated on existing and new threats that may be lurking on the ever changing internet and new users going online for the first time need to be guided through some basic awareness of things to look out for.

To compound this issue, the very nature of the applications that run on the internet evolve and take new forms which then introduce potentially new vulnerabilities. As new applications arise, new threats and exploits follow leading to a new cycle of monitoring and education which will be necessary. The ability to monitor and educate users will become key to combating the rise of cybercrime.

A global example where cybercrime education is being revisited is the United States. US President Obama’s Cyber Security Review indicates a new education plan for cyber threats in the public education system. Also, it calls for inter-jurisdictional coordination but *not* international co-operation. The latter is key as the very nature of threats have no borders, and often contain components / attack vectors from multiple regions across the globe.

Lastly, for measures like software updates, patch management, phishing education, etc, the consensus in the security industry is that consumers are not educated nearly enough when it comes to such threats. A consistent and unwavering approach will be required to keep the awareness cybercrime in mind and what to look out for.

Measures to Combat Cybercrime

To combat the cybercriminal element, a focused approach will be required by across the public and private sectors. As mentioned previously, constant education of consumers are required in order to keep awareness high and avoid significant exploitation.

Legislative and regulatory initiatives will need to bend and flex to the dynamic nature of the internet and the criminals that inhabit it. This will require vigilant monitoring of cybercrime locally and internationally to understand it’s movements and new cycles that may be on the horizon.

Inter-jurisdiction, public and private sector will need to continue investing in information sharing and cross jurisdiction co-operation to keep on top of cybercrime threats.

Lastly, by far the most complex and difficult component is international co-operation. The internet’s very nature crosses international borders at a moments notice allowing criminals to hide with anonymity while they launch their attacks. Tracing the source of an attack is one of the more easier activities. However, convincing a foreign nation’s ISP or law enforcement officials to do something about the problem is a whole other story. Internationally, governments and law enforcement need to better co-operate on the task of tracking and stopping cybercriminal activity.

Future Initiatives & Emerging Technology

Future Initiatives

In summary, next generation threats that we are seeing online today are multi-functional and come from a variety of attack vectors. Attacks occur through e-mail and file attachments / malicious links, web sites, SEO campaigns, vulnerabilities in client side software and server side software.

Involvement of public and private sector CERT (Computer Emergency Response Teams) and law enforcement organizations in monitoring new threats will be a key component in future initiatives. This would allow for early warning of new threats on the horizon and provide time for new measures and initiatives to be put in place.

A key metric for the success of future initiatives will be the timeliness of response from the public and private sector organizations as well as the governments ability to facilitate international co-operation in stamping out remote and distributed attacks.

Emerging Technologies

Criminals executing their activities online rely heavily on Trojans and Botnets. Trojans / botnets communicate subversively through common channels, sometimes with the use of encryption. Therefore, the best approach to mitigate these risks are unified and consolidated defenses. Unified defenses applying a layered security approach in which different defenses are engaged as required based on the communications being observed. This consolidate approach allows organizations to effectively counter threats very cost effectively with out compromise.

The main advantage of this approach is that it blocks the many different channels and levels in which threats occur, is scalable, centrally managed, and most importantly addresses security concerns on both the client and server side.

Future Initiatives & Emerging Technology…

Securing these two components is vital to address next generation threats. Here are some emerging technologies which will help combat these risks:

Desktop Security Software

Vendors today are already beginning to consolidate defensive measures by unifying different functions into a single package. Common software packages today provide firewall, email, anti-virus, anti-spyware protection.

Further enhancements to this are on the horizon to include web and content filtering, unifying anti-malware detection and reputation based filtering of online websites.

In addition, many internet service providers are evaluating “cloud security” models where consumers are offered “clean” internet services for a nominal fee. In this design, the service providers would provide layered security for the end user effectively sheltering them from illicit and malicious content on the internet.

Internet Access & System Security

There are several layers of security required to defeat common threats on the internet today. Individuals, gateways & access points, messaging systems and web sites & applications are all vulnerable points which need to be protected online.

Internet security software and hardware vendors are continually researching and attempting to stay one step ahead. Many challenges today involve be able to scale systems to the meet the increased demand of users and bandwidth available on the internet. Leading vendors have been able to deliver significant results by hardware accelerating and optimizing analysis and scanning components to better meet the demands of the growing networks. Further and continual investment will be required from public and private sector organizations to research and develop new ways of combating online threats.

Appendix

Initiatives

National E-security Awareness Week 2009
http://www.staysmartonline.gov.au/awareness-week

Cyber Storm III
http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~Cyber+StormIII+Fact+Sheets+V3.PDF/$file/Cyber+StormIII+Fact+Sheets+V3.PDF

ISP Level Content Filtering Trials
http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf

Online Resources

http://www.staysmartonline.gov.au/

http://www.scamwatch.gov.au/

Internet related Government Departments

The Department of Broadband, Communications and the Digital Economy
http://www.dbcde.gov.au/ -

Australian Communications and Media Authority
http://www.acma.gov.au/WEB/LANDING/pc=INTERNET_MAIN

The Australian Government Information Management Office
http://www.finance.gov.au/agimo/index.html

National Security and Criminal Justice Group (E-Security Policy and Coordination Branch)
http://www.ag.gov.au/www/agd/agd.nsf/Page/Organisational_StructureNational_Security_and_Criminal_JusticeSecurity_and_Critical_InfrastructureE-Security_Policy_and_Coordination_Branch

Online References

Obama to learn results of cyber security review
http://www.australianit.news.com.au/story/0,,25360722-24170,00.html

McColo
http://en.wikipedia.org/wiki/McColo

Thank You.

www.fortinet.com